Dunn S, Wilkinson S.

Hazard Tolerance of Spatially Distributed Complex Networks.

***Reliability Engineering and System Safety* 2017, 157, 1-12.**

Reliability Engineering and System Safety 157 (2017) 1–12

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Hazard tolerance of spatially distributed complex networks

Sarah Dunn *, Sean Wilkinson

Newcastle University, Newcastle, UK

ARTICLE INFO

Article history:
Received 12 February 2016
Received in revised form
4 August 2016
Accepted 15 August 2016
Available online 18 August 2016

Keywords:
Network theory
Spatial networks
Resilience
Reliability
Infrastructure systems
Spatial hazard

ABSTRACT

In this paper, we present a new methodology for quantifying the reliability of complex systems, using techniques from network graph theory. In recent years, network theory has been applied to many areas of research and has allowed us to gain insight into the behaviour of real systems that would otherwise be difficult or impossible to analyse, for example increasingly complex infrastructure systems. Although this work has made great advances in understanding complex systems, the vast majority of these studies only consider a systems topological reliability and largely ignore their spatial component. It has been shown that the omission of this spatial component can have potentially devastating consequences. In this paper, we propose a number of algorithms for generating a range of synthetic spatial networks with different topological and spatial characteristics and identify real-world networks that share the same characteristics. We assess the influence of nodal location and the spatial distribution of highly connected nodes on hazard tolerance by comparing our generic networks to benchmark networks. We discuss the relevance of these findings for real world networks and show that the combination of topological and spatial configurations renders many real world networks vulnerable to certain spatial hazards.

1. Introduction

Infrastructure systems, including water, electricity, transportation and telecommunication, are of critical importance to our modern communities. The reliability of these physical assets and the services they provide are vital for ensuring national security, public health and productivity [20]. It is therefore no surprise that the reliability of these systems has received a great deal of attention in recent years [23]. However, these systems are becoming increasingly complex and interdependent, meaning that they now rely on each other to function normally [15,21], and this increased complexity and reliance is making these networked infrastructure systems harder to manage and assess [33]. We therefore require new tools and techniques to assess their reliability. One possible solution is to use a network graph theory approach to quantify the reliability of these complex infrastructure systems.

Network graph theory has previously been used to analyse a range of systems and provides a rigorous mathematical basis for the analysis of connected elements, enabling aspects of aggregate performance of networked systems to be rapidly calculated [10]. Network models are being increasingly used to improve our understanding of: social systems [2,26,3], neural networks [35,36,6], biological networks [34] and computer science systems [37], amongst others. Studies applying network theory to real-world systems, have recently turned from the analysis of social and biological networks, where space is not traditionally a governing factor, to the analysis of infrastructure systems, which can be distributed over vast geographic regions [14,16,28]. In the case of infrastructure systems, it has been assumed that because many of these networks have been shown to be topologically resilient to a random hazard (e.g. a reliability failure of individual components) they are also resilient to spatially dispersed random hazards (e.g. snowstorm, windstorm). However, Wilkinson et al. [38] analysed the impacts of the Eyjafjallajökull volcano to the European Air Traffic Network and found that this network showed a surprising vulnerability to this hazard, contradicting its assumed topological hazard tolerance. They found that this vulnerability was due to a combination of its topological characteristics and geographical distribution of airports in the network, which is not accounted for in traditional network theory studies, which only consider network topology. The little research that has analysed real-world spatial networks (e.g. infrastructure systems) focuses mainly on characterising the topology of the system, while the spatial element of the same network receives less attention - if not neglected entirely [5]. There are a few studies that have considered the "spatial" resilience of interdependent gas and electrical networks [29,31] or the resilience of China air traffic network [24,30], for example. However, all of these studies have assessed specific real-world applications of spatial resilience and have not considered the overarching, or inherent, resilience of spatial networks in general.

In this paper, we aim to give an assessment of the spatial

* Corresponding author.
E-mail address: sarah.dunn@ncl.ac.uk (S. Dunn).

http://dx.doi.org/10.1016/j.ress.2016.08.010
0951-8320/

hazard tolerance of a range of complex networks, in a similar manner to the study by Albert et al. [1] who considered topological resilience. To achieve this, we provide a robust framework that can quantify the reliability of a complex system to a range of spatial hazards. Unlike previous spatial hazard studies, we do no focus solely on one real-world system but instead generate a range of synthetic networks (termed 'benchmark networks') to use in our resiliency testing. However, we do show that these benchmark networks are characteristic of real-world systems and relate our findings from the 'benchmark networks' to these real-world systems. We consider three classes of relational network model (random, scale-free and exponential networks) which are combined with two different spatial nodal configurations and assess their hazard tolerance to two different locations of a 'growing' spatial hazard.

The rest of the paper is structured as follows: in Section 2, the paper considers the spatial nodal configuration of the 'benchmark networks' and Section 3 considers their network class (i.e. topology). Section 4 develops the spatial hazard models to be used to in our analysis, to which our 'benchmark networks' are then subjected in Section 5. Finally, Section 6 provides conclusions and ideas for future research.

2. Nodal configuration

There has been very little research into the nodal locations of real-world networks. The majority of previous research has investigated pre-existing real-world networks and has therefore used the actual nodal locations [17], or has used purely topological models [17,18,7]. The location of nodes within a real-world network is a very complex problem. In the case of real world systems, nodes may represent cities, regions within cities or individual infrastructure components. Furthermore these systems are dynamic, evolving over time in response to a myriad of drivers such as demographic shifts, technological advancement and availability of resources. Therefore, we generate a range of generic nodal locations and use these to form spatial 'benchmark networks' for testing resiliency. These benchmarks capture the overall distribution of nodes in geographical networks, but not necessarily the small scale local areas of high density nodes (e.g. the model will capture the spread of airports over a continent, but not necessarily the high density of airports clustered around a population centre). This allows us to draw conclusions on the overall hazard tolerance of spatial networks, in a similar manner to traditional topological hazard assessments.

In this paper, we simulate two different spatial nodal layouts and contain them within a 'spatial boundary', outside which no nodes are allowed to form. In the case of a real-world network, this spatial boundary could represent the extent of a land boundary or air space in the case of an air traffic network. We are considering generic spatial layouts in this paper, rather than simulating one area in particular, and have therefore chosen to enclose the networks in a circular boundary. The two different spatial nodal layouts used in this paper are:

- *Uniform with distance* (Fig. 1(a)) – the number of nodes increases linearly with distance away from the geographic centre of the network
- *Uniform with area* (Fig. 1(b)) – the nodes are spread evenly over the network.

The spatial distributions for the two nodal layouts are shown in Fig. 1. These distributions plot the number of nodes against distance from the geographic centre. From this figure, it can be seen that the uniform with distance configuration shows a linear relationship between the proportion of nodes and the distance from geographical centre, whereas the uniform with area configuration exhibits a quadratic relationship.

3. Network classes and models

Relational network models do not include a spatial component, therefore we modify the traditional generation algorithms of random, scale-free and exponential networks to generate a range of spatial networks. All of the generated networks used in this paper have 500 nodes and approximately 3200 links. We have chosen to generate scale-free and exponential networks as they have been shown to capture the real-world characteristics of many infrastructure systems (for example: [32,39]). Whilst, random networks are often used in tests of network robustness to determine if a more structured network is resilient or vulnerable to the applied hazard, due to the homogeneous nature [22,25].

3.1. Random network

In this paper, we generate the random networks using the algorithm of Erdos and Renyi [13]. In this generation algorithm, each pair of nodes is considered in turn and a connection (link) is made between them based upon a value of linking probability (the higher this value the more likely it is that a link will be generated). If the linking probability is equal to 1, then the network will be saturated (i.e. it will have the maximum possible number of links) and if this value equals 0 there will be no links in the network. We do not modify this generation algorithm to take into account the spatial distance between nodes as we are not seeking to create the most efficient network possible (i.e. we are not seeking to minimise, or maximise, the distances between pairs of nodes). In this paper, we are using the random network as a benchmark for tests of resilience for the other two more sophisticated network classes and therefore choose the linking probability to result in approximately the same number of links as these two networks (around 0.025, which results in a network with approximately 3200 links). The degree distributions for the generated networks can be seen in Fig. 2(a) and the associated spatial degree distributions are shown in Fig. 2(b).

3.2. Scale-free network

The scale-free network was first identified and developed by Barabasi and Albert [4] and is based upon the ideas of *growth* and *preferential attachment* [5]. These networks are formed by starting with an initial number of isolated nodes, m_0, which is usually a small percentage of the total number of nodes in the network. New nodes are then added to the network at each 'time step' (i.e. 'growing' the network) until the total number of nodes in the network is reached. These added nodes have between 1 and m_0 links attached to them and connect to the existing nodes in the network based upon the idea of 'preferential attachment'. The probability of attaching to each existing node is calculated based upon its degree, with the nodes with a high degree being more likely to 'attract' a link from the new node (i.e. the rich get richer). It is this 'preferential attachment' rule which results in a few high degree nodes and many small degree nodes in the network. If a spatial layout of the network as nodes are introduced into the network those nodes that are introduced early in the process have more chance to 'attract' links from other nodes compared to nodes introduced later to the network and are therefore more likely to have a higher degree than those introduce late, which in turn has a significant impact upon their spatial hazard tolerance [11].

Therefore we study three methods of choosing the introduction

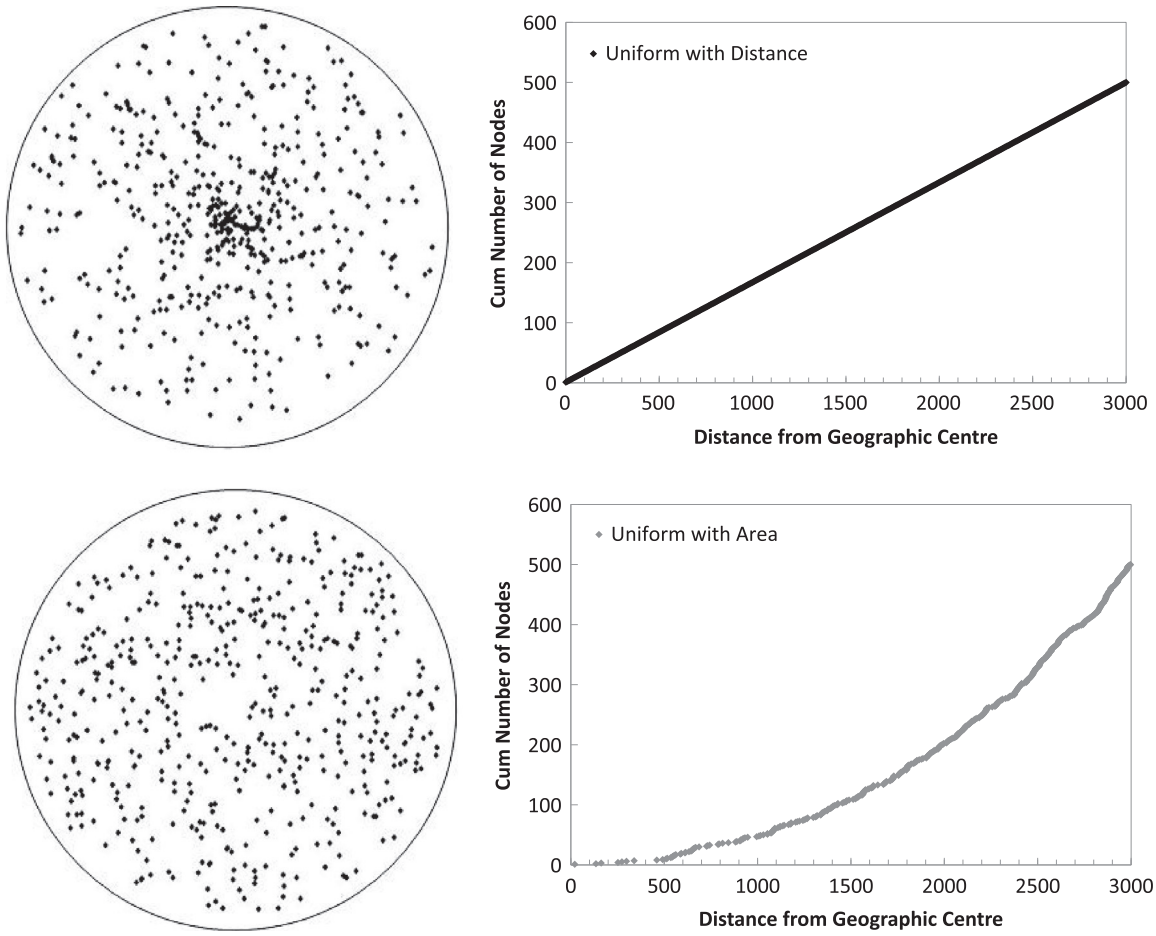

Fig. 1. Showing the (a) *uniform with distance* nodal configuration, (b) its associated spatial distribution and also (c) the *uniform with area* nodal configuration and (d) its associated spatial distribution.

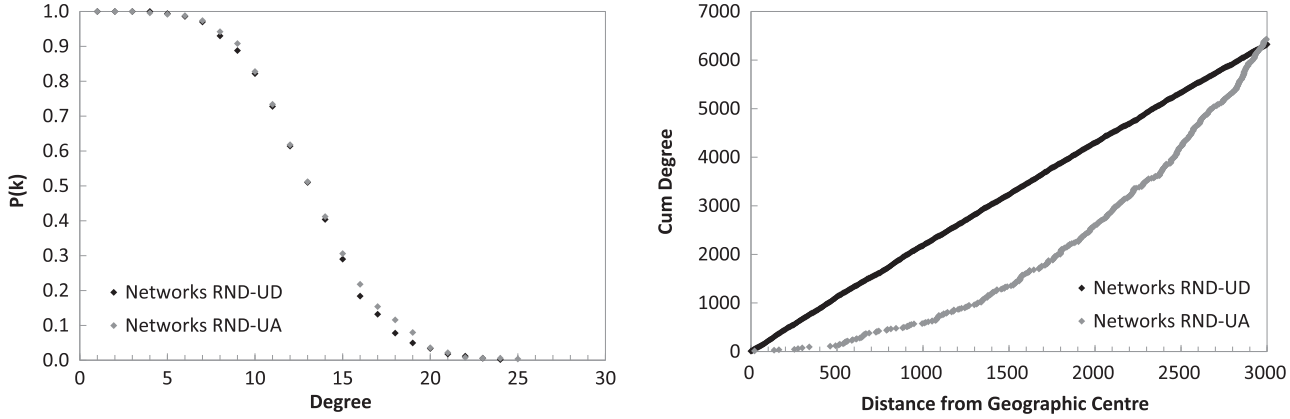

Fig. 2. Showing the (a) degree distributions and (b) spatial degree distributions for the random networks with a uniform with area and uniform with distance nodal layout. The reader is referred to Table 1 for an explanation of the legend used in this figure.

order of the nodes in the scale-free network models, these are:

- *Random* – the node location does not affect the order in which nodes are added to the network (i.e. it is completely random).
- *Distance from the geographic centre* – nodes are introduced shortest to furthest distance away from the geographic centre (i.e. midpoint) of the network.
- *Proportional to distance from the geographic centre* – similar to previous, with the exception that all nodes are assigned a probability value (with those in the centre of the network having the highest probabilities) and are introduced based on this value. Nodes in the centre of the network are more likely to be chosen to be introduced first.

The different spatial distributions, resulting from the three different node introduction orders, can be seen in Fig. 3(b) and (d) and also shown visually on a sample network in Fig. 4. From these figures, it can be seen that networks where nodes were introduced with distance from the geographic centre show a greater proportion of high degree nodes around the centre of the spatial domain (Fig. 4(a)), when compared to networks were the nodes were introduced randomly (Fig. 4(c)). This is expected as these

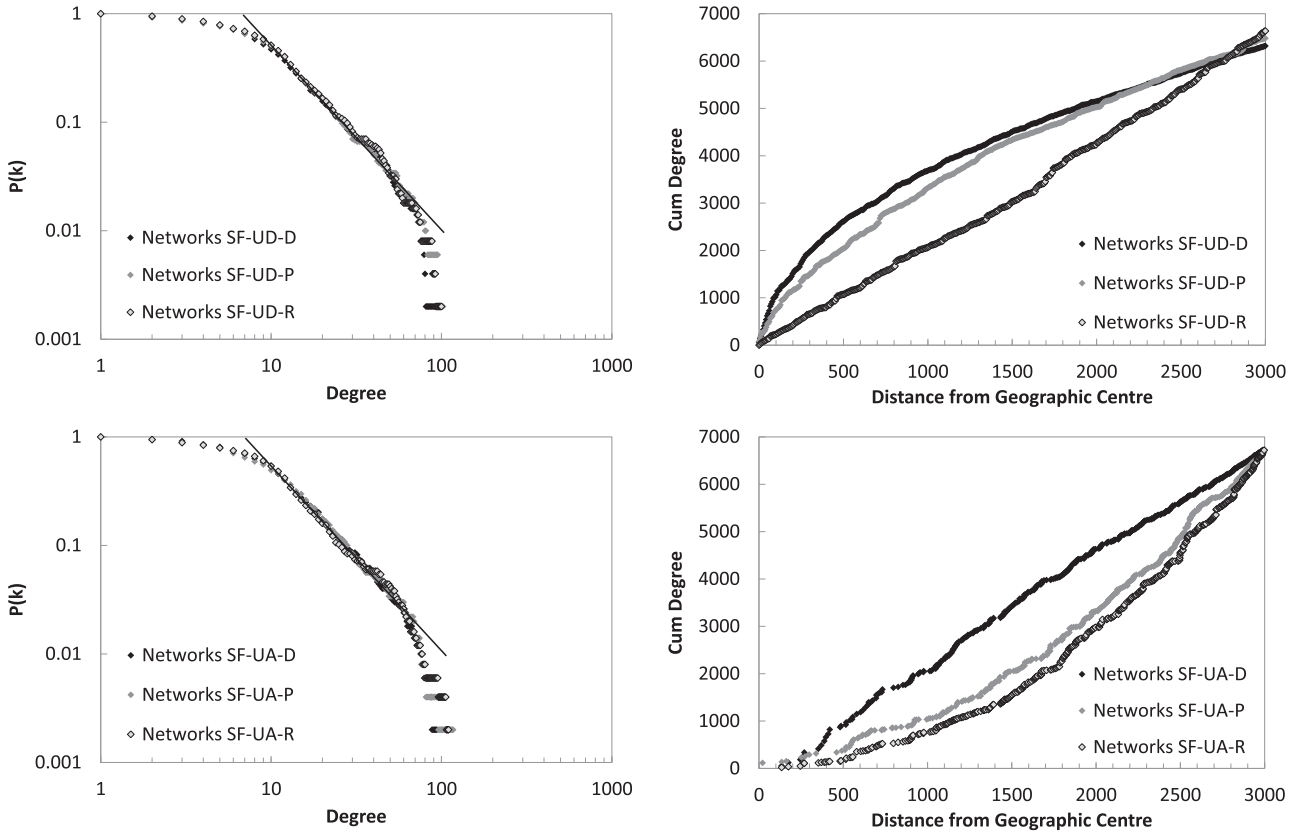

Fig. 3. Showing the (a) topological degree distributions and (b) spatial degree distributions for the scale-free networks with a uniform with distance nodal layout, and also showing the (c) topological degree distributions and (d) spatial degree distributions for the scale-free networks with a uniform with are nodal layout. In all cases, the three nodal introduction orders are shown (with distance from the geographic centre, proportional to distance from the geographic centre and randomly). The reader is referred to Table 1 for an explanation of the legend used in this figure.

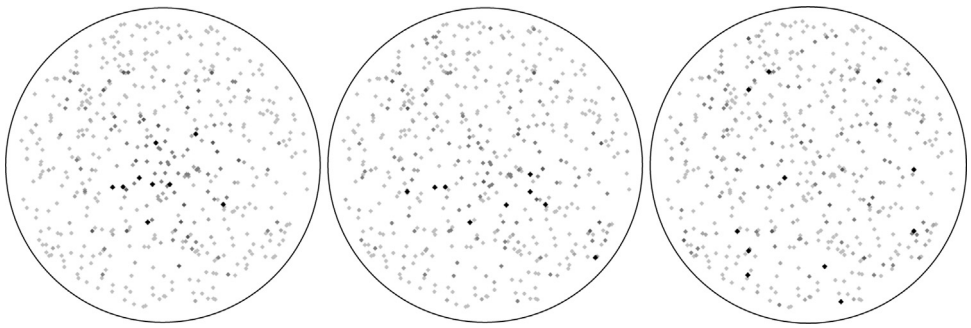

Fig. 4. Three scale-free networks with a uniform with area nodal layout, where the nodes are introduced to the network: (a) with distance from the geographical centre, (b) proportion with distance from the geographic centre, and (c) randomly. The spatial boundary is shown as a black circle and the nodes are shown as grey-scale dots. The colour of the node indicates its degree, with black nodes having a high degree and light grey nodes a low degree. The links between the nodes have been omitted for clarity.

nodes have been introduced to the network in an early 'time step' and have therefore had more chances to attract links from nodes that were introduced at a later 'time step'. In contrast, the high degree nodes in the network where the nodes have been introduced randomly are more spatially dispersed over the whole layout of the network, with the proportion to distance layout exhibiting behaviour in between these two extremes. It is also interesting to note that the degree distributions for all of the scale-free networks are approximately the same (Fig. 3(a) and (c)).

3.3. Exponential network

The exponential network class is not as well documented as the other classes of network model; however, one model to create exponential networks with a spatial component does exist, developed by Wilkinson et al. [38]. This algorithm is based on the scale-free network model [4], but with the modification that allows low degree nodes capitalise on their close proximity to high degree nodes and attract links that were bound for the high degree node. Following Barabasi and Albert [4], the algorithm starts with an initial number of starting nodes, m_0, and the remaining nodes are added individually to the network. Similarly to the scale-free model, each new node added has between 1 and m_0 links attached to it, which it uses to preferentially attach to the existing network. However, this preference is now based on the degree of all nodes within the 'neighbourhood' of the node we are attempting to attach to, rather than that of individual nodes, which is set by assigning a radius, r. Setting the radius to zero removes the spatial dependence of the network resulting in a scale-free network, while setting the radius to twice the size of the

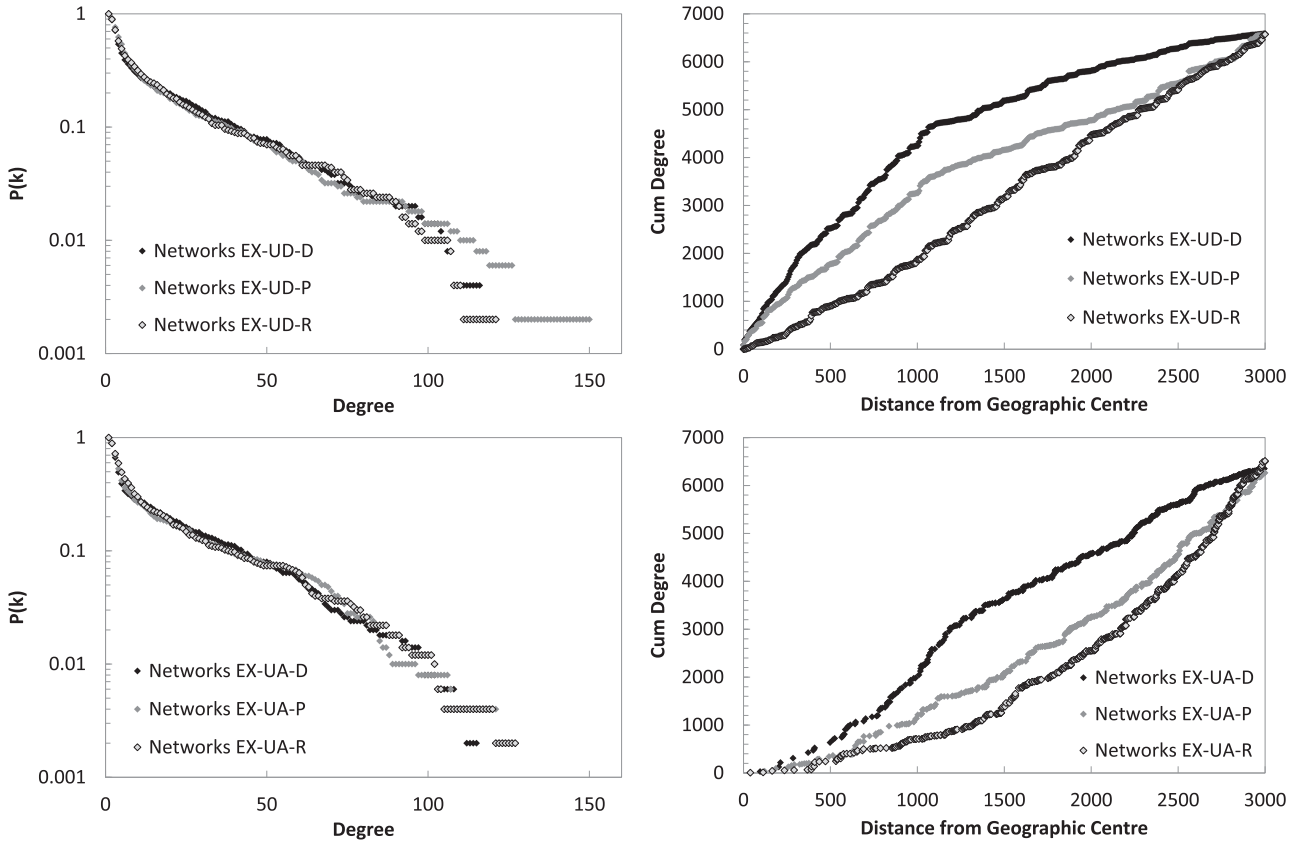

Fig. 5. Showing the (a) degree distributions and (b) spatial degree distributions for the exponential networks with a uniform with distance nodal layout, and also showing the (c) degree distributions and (d) spatial degree distributions for the exponential networks with a uniform with are nodal layout. In all cases, the three nodal introduction orders are shown (with distance from the geographic centre, proportional to distance from the geographic centre and randomly). The reader is referred to Table 1 for an explanation of the legend used in this figure.

spatial domain results in random attachment. We generate the networks in this paper using the algorithm of Wilkinson et al. [38], using the value of $r=0.25$; the resulting degree distributions are shown in Fig. 5(a) and (c). It is worth noting that strictly speaking this network is in fact a truncated scale-free network as described by Guimera et al. [19] but could with equal validity be called an exponential network with a scale-free tail. For convenience and to distinguish them from scale-free networks, in this paper we will refer to them as exponential networks.

Similar to the scale-free networks, the order in which nodes are introduced to the network impacts upon the spatial location of the high degree nodes and therefore affects the spatial hazard tolerance of the network. To investigate this impact we use the same three methods of node introduction order as used for the scale-free networks. The resulting spatial degree distributions are shown in Fig. 5(b) and (d), where it can again be seen that introducing nodes in order of distance from the geographic centre results in a greater proportion of high degree nodes in this area, compared to introducing nodes randomly.

3.4. 'Benchmark Network' summary

In this paper, we use the three network generation algorithms and two spatial nodal configurations to generate a total of 140 'benchmark networks' outlined in Table 1.

3.5. Real-world infrastructure characteristics

In this paper, we have generated a range of spatial networks which we intend to use for resilience testing. To show that these synthetic networks are characteristic of real-world infrastructure systems we have collected and analysed the topological and spatial properties of a series of real-world datasets of different sizes and scales, shown in Table 2. We assess their topological properties in terms of the degree distribution and consider their spatial properties by plotting the spatial distribution (which is obtained by plotting the distance from the weighted geographic centre against the number of nodes within this radius) and spatial degree distribution (similar to the spatial distribution, but plots the sum

Table 1
Showing the number networks created and analysed for each network class, nodal configuration and node introduction order. It is worth noting that random networks are unaffected by node introduction order, as decisions to connect pairs of nodes (via links) are independent of any spatial influences.

Network	Spatial nodal configuration	Node introduction order		
		Randomly (R)	Distance (D)	Proportional with distance (P)
Scale-Free (SF)	Uniform with Distance (UD)	10	10	10
	Uniform with Area (UA)	10	10	10
Exponential (EX)	Uniform with Distance (UD)	10	10	10
	Uniform with Area (UA)	10	10	10
Random (RND)	Uniform with Distance (UD)	10		
	Uniform with Area (UA)	10		

Table 2
Showing the topological and spatial characteristics of a number of real-world infrastructure systems. The data regarding the three air traffic networks was obtained from [27], the UK National Grid data was obtained from the RESNET project (see Acknowledgements), the UK rail network was obtained from [9] and the US rail network and highway network were obtained from [8]. The reader is referred to Table 1 for an explanation of the legend used in this figure.

Network	Number of nodes/links	Degree distribution	Spatial distribution	Spatial degree distribution	Synthetic proxy
European Air Traffic Network	525/3886	Exponential	Uniform with Distance	Uniform with Distance	EX-UD-D
US Air Traffic Network	363/2289	Exponential	Uniform with Area	Uniform with Area	EX-UA-P
China Air Traffic Network	124/828	Exponential	Uniform with Distance	Uniform with Distance	EX-UD-D
UK National Grid	218/278	Exponential	Uniform with Distance	Uniform with Distance	EX-UD-D
UK Rail Network	4095/5942	Exponential	Uniform with Area	Uniform with Area	EX-UA-D
US Rail Network	24,038/27,768	Exponential	Uniform with Distance	Uniform with Distance	EX-UD-P
US Highway Network	74,027/111,936	Scale-Free	Uniform with Distance	Uniform with Distance	SF-UD-R

of the degree of all nodes within the given radius). For a more detailed, and graphical, explanation of these measures the reader is directed to Dunn et al. [12].

In Table 2 the synthetic network to which these real-world systems most closely align has also been identified. It is acknowledged that many of these real-world systems do not follow the exact 'smooth' spatial distribution of the synthetic networks, as they can show slight distortions due to the local clustering of nodes (for example, the UK rail network shows a disproportionately high number of stations clustered around London, when compared to the rest of the UK).

4. Spatial and topological hazard scenarios

In this paper, we simulate a range of hazards, aiming to assess the hazard tolerance of the networks to a variety of different 'attacks'. Two of the hazards have a spatial component and two are topological. We will later demonstrate that adding a spatial element to our network generation algorithms does not alter the topological behaviour of these networks. We subject the networks to a topological degree attack (removing nodes in order of their degree from highest to lowest) and a topological random hazard (removing nodes randomly from the network). The two spatial hazards that we use in this paper are:

- *'Central attack'* (Fig. 6(a)–(c)) – the centre of the hazard is fixed at the geographic centre of the network and the size of the hazard is increased.
- *'Perimeter attack'* (Fig. 6(d)–(f)) – the centre of the hazard is fixed at a point on the spatial boundary of the network and the size of the hazard is increased.

In the spatial hazard analysis, we remove nodes, and their connecting links, from the network as they are impacted by the spatial hazard (e.g. as they are covered by the grey circles in Fig. 6).

In this paper, we have chosen to apply our developed methodology to assess the disruption caused by spatial hazards, as this element of network theory is usually neglected in studies of real-world systems [5]. However, we could equally have chosen to apply this methodology to the analysis of random nodal failure or sought to remove nodes with poor reliability ratings from the network and quantified this impact. The same methodology can be utilised by simply changing the order in which nodes (and their connecting links) are removed from the network (e.g. removing nodes in order of their reliability rating).

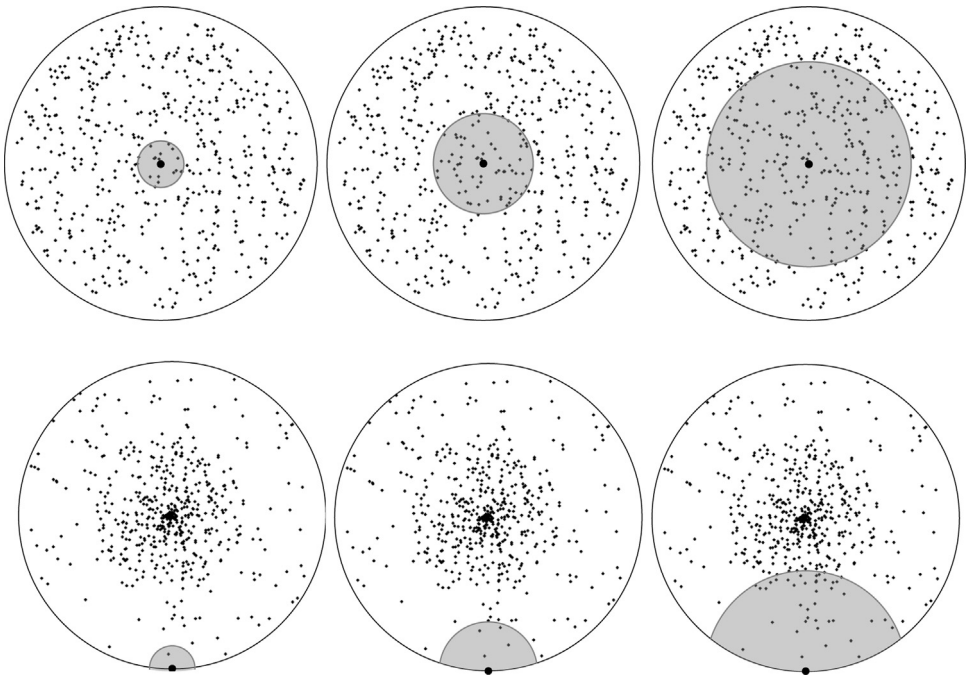

Fig. 6. Showing the growing (a–c) 'central attack' and (d–f) 'perimeter attack' spatial hazards, overlaid on a nodal layout; where the nodes are indicated by the black dots and the spatial boundary as a black circle. The hazard centre is shown using a large black dot (for all hazards), from which the hazard grows (grey circle) until it covers the whole network area.

5. Results and discussion

There is a large combination of results that could be presented from the analysis, therefore, to keep this section, and the paper, to a manageable length we focus on three main research questions. Firstly, we consider the impact that node introduction order has to the resulting hazard tolerance of the spatial scale-free and exponential networks; secondly, we consider the impact that nodal configuration has to hazard tolerance and finally, we consider the combinations of hazard, node introduction order and nodal configuration that produces the 'worst' and 'best' resilience and compare this to the results of 'traditional' topological hazard.

We present the results in terms of the proportion of failed links and the proportion of failed nodes/area. We also quantify the reliability/resilience of networks with different characteristics using a modified version of the Relative Spatial Vulnerability Index (RSVI) of Li et al. [24], which is a formalised measure of the methodology derived by Wilkinson et al. [38], given by Eq. (1). The original RSVI calculates the percentage change in the area between the sophisticated network ($g(x)$) and the benchmark resilience network ($g_{BM}(x)$) when plotting the proportion of area covered by the hazard against the proportion of impacted (or removed) nodes. This results in one numerical value of resilience for the sophisticated network, when compared to the benchmark network. In this paper, we modify this approach in three ways. Firstly, we convert the value to a percentage in order to present the percentage change between the test network and the benchmark, which is a more comparable and interpretable measure of relative resilience. Secondly, for test networks that show both resilience and vulnerability, compared to the benchmark network, we do not use one value of this measure but rather calculate the RSVI for each section (i.e. one value for the vulnerable section and one for the resilient section). We make note of where the test network intersects the benchmark (i.e. the point where it has the same hazard tolerance) and use this point to define the limits i and j (in Eq. (1)) setting the range with which the resilience, or vulnerability, is considered. It is worth noting that for a network which is entirely resilient or vulnerable, when compared to the benchmark network, i and j equate to 0 and 1 respectively. We make this distinction in order to gain further insight into the magnitude of the vulnerability and resilient components and also to highlight the point at which the network switches from vulnerable to resilient, or vice versa. Finally, we reverse the sign of the original RSVI measure, in order to generate a negative value for networks that are more vulnerable compared to the benchmark and a positive value for networks that are more resilient. We do this to ensure the output value is not misinterpreted.

$$\mathrm{RSVI}_{\mathrm{modified}} = \int_i^j \left(\frac{g(x) - g_{BM}(x)}{g_{BM}(x)} \right) dx \times -100\% \tag{1}$$

In addition to this measure, we also quantify the initial gradient of the networks (when plotting the proportion of closed nodes/area against removed links) to determine their resilience to small scale spatial disruptions.

5.1. Impact of node introduction order

We initially identify the impact that node introduction order has to the hazard tolerance of the scale-free and exponential networks, when compared to the random benchmark networks. In this analysis we consider the *uniform with distance* and *uniform*

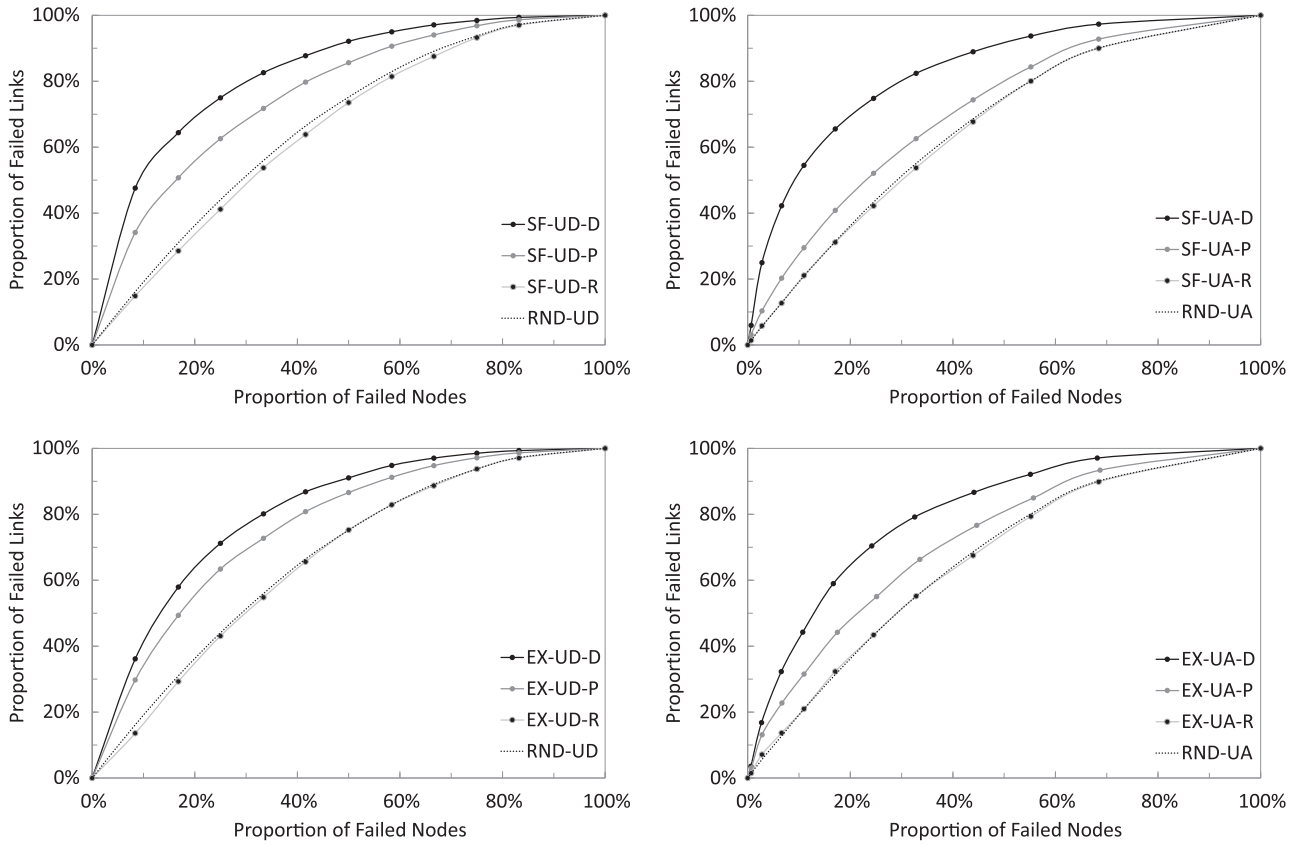

Fig. 7. Showing the hazard tolerance of scale-free networks with (a) uniform with distance and (b) uniform with area nodal layouts, when plotted in terms of the proportion of failed nodes by the growing 'central attack' spatial hazard and the proportion of failed links. Also showing the same results for the exponential networks with (c) uniform with distance and (d) uniform with area nodal layouts. In all graphs the random benchmark networks, with the corresponding nodal configuration, are also shown. The reader is referred to Table 1 for an explanation of the legend used in this figure.

Table 3
Quantification of the resilience of scale-free networks (shown in Fig. 7(a) and (b)), with either a uniform with distance (UD) or uniform with area (UA) nodal configuration, with regards to random benchmark networks with the same nodal configuration. The reader is referred to Table 1 for an explanation of the legend used in this table.

Network	Modified RSVI	Initial Gradient
SF-UD-D	−24.18%	5.66
SF-UD-P	−14.63%	4.06
SF-UD-R	+2.09%	1.77
RND-UD	–	1.92
SF-UA-D	−24.15%	8.99
SF-UA-P	−6.82%	3.72
SF-UA-R	+0.70%	2.09
RND-UA	–	2.02

Table 4
Quantification of the resilience of exponential networks (shown in Fig. 7(c) and (d)), with either a uniform with distance (UD) or uniform with area (UA) nodal configuration, with regards to random benchmark networks with the same nodal configuration. The reader is referred to Table 1 for an explanation of the legend used in this table.

Network	Modified ASVI	Initial Gradient
EX-UD-D	−20.66%	4.30
EX-UD-P	−14.20%	3.54
EX-UD-R	−0.24%	1.62
RND-UD	–	1.92
EX-UA-D	−19.74%	6.23
EX-UA-P	−8.06%	4.69
EX-UA-R	+0.34%	2.56
RND-UA	–	2.02

with area nodal configurations when subjected to the 'central attack' spatial hazard (Fig. 6(a)–(c)). The results of this analysis are shown in Fig. 7, where we plot the proportion of failed nodes against the proportion of failed links.

The results, presented in Fig. 7 and Tables 3 and 4, show that the spatial hazard tolerance of the networks is largely governed by the location of the high degree nodes in the network. The synthetic networks where the nodes have been introduced with distance, and consequently have the majority of high degree nodes are located around the geographic centre of the network (see Fig. 4), show a high vulnerability to hazards located over this area. Whereas, networks where the nodes have been introduced randomly, and therefore have a dispersion of high degree nodes, show approximately the same resilience as the random benchmark networks. These results are to be expected when considering the location of the high degree nodes, however, this expectation does not provide a means to quantify the change in resilience. This is achieved from the modified RSVI measure, which shows that the networks with a spatial dispersion of nodes are approximately 24% more resilient than networks with a cluster of high degree nodes. The initial gradient of the networks also shows this increase in vulnerability, with the gradient of the networks with a cluster of high degree nodes being more than 3 times greater than that of networks with spatially dispersed high degree nodes.

5.2. Impact of spatial nodal configuration

We now consider the impact that the nodal configuration has to the resilience of the scale-free and exponential networks, when compared to the random benchmark networks. In this analysis, we consider both the uniform with distance and uniform with area nodal configurations, but only the random node introduction order (to negate the impact that the placement of high degree nodes has to the hazard tolerance, as shown in the previous section) and subject these networks to both the 'central attack' and 'perimeter attack' spatial hazards. The results of this analysis are plotted in Fig. 8, in terms of the proportion of closed area (i.e. the proportion of area affect by the spatial hazard) and the resulting proportion of failed links. From this figure, it can be seen that the results for the scale-free and exponential networks are very similar to that of the random benchmarks and therefore the quantification using the modified RSVI measure is not presented in this case (but for all networks is calculated to be in the range of a 0–1.5% change in resilience). The initial gradient for these results are presented in Table 5.

From these results, it can be seen that the geographic nodal configuration is also a governing factor in determining the resilience of the network. Focusing on the 'central attack' spatial hazard (Fig. 8(a) and (c)), it can be seen that networks with a uniform with distance nodal configuration show the most vulnerability, for all sizes of hazard. This difference in vulnerability is quantified using the modified RSVI measure, shown in Table 6, where it can be seen that the networks with a uniform with distance nodal configurations are approximately 26% more vulnerable to the 'central attack' spatial hazard than those with a uniform with area configuration. This increased vulnerability is also shown by the increased initial gradient values (Table 5) and is due to the presence of a large proportion of nodes around the geographic centre in the uniform with distance configuration (Fig. 1(a)), meaning that for only a small hazard size a large proportion of nodes are removed.

In contrast to this vulnerability, the high proportion of nodes clustered around the centre of the network in the uniform with distance nodal configuration, causes the networks show resilience to small hazards located at the perimeter of the network (Fig. 8 (b) and (d)). These networks are around 19% more resilient than those with a uniform with area configuration for small sizes of spatial hazard, covering up to 35% of the spatial area of the network (Table 7). After this point, the networks with a uniform with distance configuration show increasing vulnerability and are approximately 12% more vulnerable than the networks with a uniform with area configuration.

5.3. Impact of spatial hazard vs. impact of topological hazard

In this section, we compare the impacts that both spatial and topological hazards have on the networks. We consider the combinations of nodal configuration, node introduction order and spatial hazard that produce the most vulnerable network (referring to this as the 'worst case' scenario) and the most resilient network (referring to this as the 'best case' scenario). We compare the 'worst case' scenario to the topological degree attack, as both scale-free and exponential networks have been shown to be inherently vulnerable to this attack strategy. And we compare the 'best case' scenario to the topological random hazard, as these network classes have been shown to be inherently resilient to this hazard. The results of this analysis and comparison to the best and worst case spatial networks (Fig. 8) are shown in Fig. 9, in terms of the proportion of nodes removed against the proportion of links removed.

Considering the 'worst case' scenarios, Fig. 9 shows that both the scale-free and exponential networks are more vulnerable to the topological degree attack than the 'central attack' spatial hazard, which is quantified using the modified RSVI measure in Table 8. These results show that the 'worst case' network combination is between 5% and 13% more resilient to the spatial hazard than the topological attack. Whilst there is a high proportion of high degree nodes located around the centre of the network (which are removed first by the 'central attack' spatial hazard) there are still some lower degree nodes present in this area (see

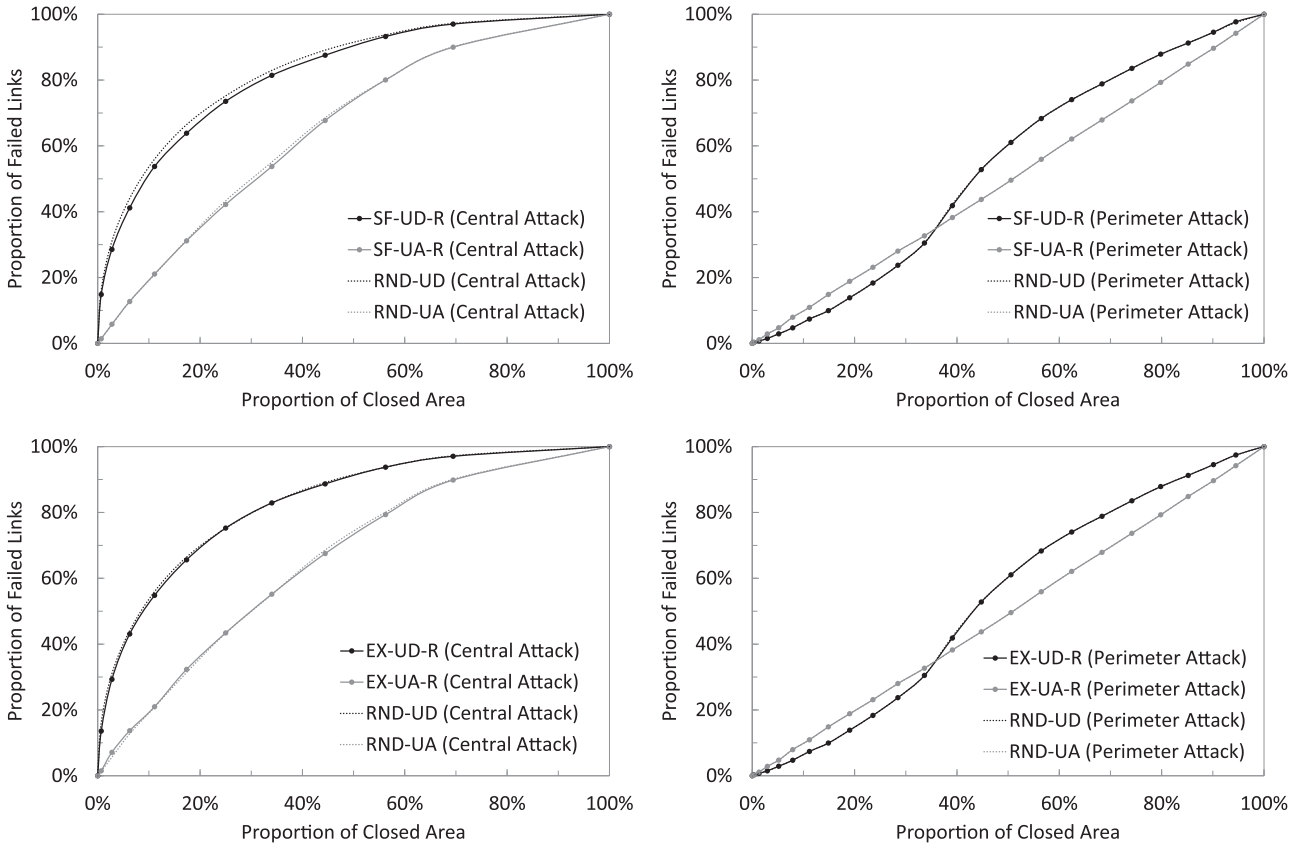

Fig. 8. Showing the hazard tolerance of scale-free networks with uniform with distance and uniform with area nodal layouts, when subjected to (a) 'central attack' and (b) 'perimeter' spatial hazards, with the results plotted in terms of the proportion of area closed (or covered) by the growing spatial hazard. Also showing the same results for the exponential networks with a uniform with distance and uniform with area nodal layouts when subjected to the (c) 'central attack' and (d) 'perimeter' spatial hazards. In all graphs the random benchmark networks are also shown, but may be difficult to distinguish as they have the same results as the scale-free and exponential networks with the same nodal configuration. The reader is referred to Table 1 for an explanation of the legend used in this table.

Table 5
Quantification of the initial gradient of the scale-free and exponential networks, shown in Fig. 8.

Network	Hazard	Initial gradient
SF-UD-R	Central attack	21.41
	Perimeter attack	0.60
SF-UA-R	Central attack	2.09
	Perimeter attack	1.00
EX-UD-R	Central attack	19.57
	Perimeter attack	0.60
EX-UA-R	Central attack	2.57
	Perimeter attack	1.00

Table 6
Comparison of the quantified resilience of scale-free and exponential networks, shown in Fig. 8(a) and (c) respectively.

Series	Modified RSVI
Resilience of SF-UD-R (central attack) compared to SF-UA-R (central attack)	−25.18%
Resilience of EX-UD-R (central attack) compared to EX-UA-R (central attack)	−26.09%

Fig. 4(a)). This causes the network to be less vulnerable to this hazard (as it will remove fewer links) than the topological degree attack as this removes nodes in order of their degree.

The 'best case' scale-free and exponential networks both show an initial resilience to the 'perimeter attack' spatial hazard

Table 7
Comparison of the quantified resilience of scale-free and exponential networks, shown in Fig. 8(b) and (d) respectively.

Series	Modified RSVI (from 0% to 35%)	Modified RSVI (from 35% to 100%)
Resilience of SF-UD-R (perimeter attack) compared to SF-UA-R (perimeter attack)	+19.53%	−11.95%
Resilience of EX-UD-R (perimeter attack) compared to EX-UA-R (perimeter attack)	+18.30%	−11.95%

compared to the topological random hazard, until 38% of nodes have been removed, shown in Fig. 9 and quantified Table 9. This is due to the large proportion of low degree nodes close to the spatial boundary of the network, which are removed first by the spatial hazard; whereas, the topological random hazard has an equal chance of removing each node in the network and will therefore tend remove the majority low degree nodes but will also remove a few higher degree nodes, causing the network to show more vulnerability to this attack strategy. However, as the spatial hazard reaches the geographic centre the network becomes increasingly vulnerable to further expansion of the hazard, causing the network to be more vulnerable to this attack strategy than the topological random hazard.

This analysis has shown that whilst the location of nodes and also the location of the high degree nodes are governing factors in determining the resilience of a network to spatial hazard, the

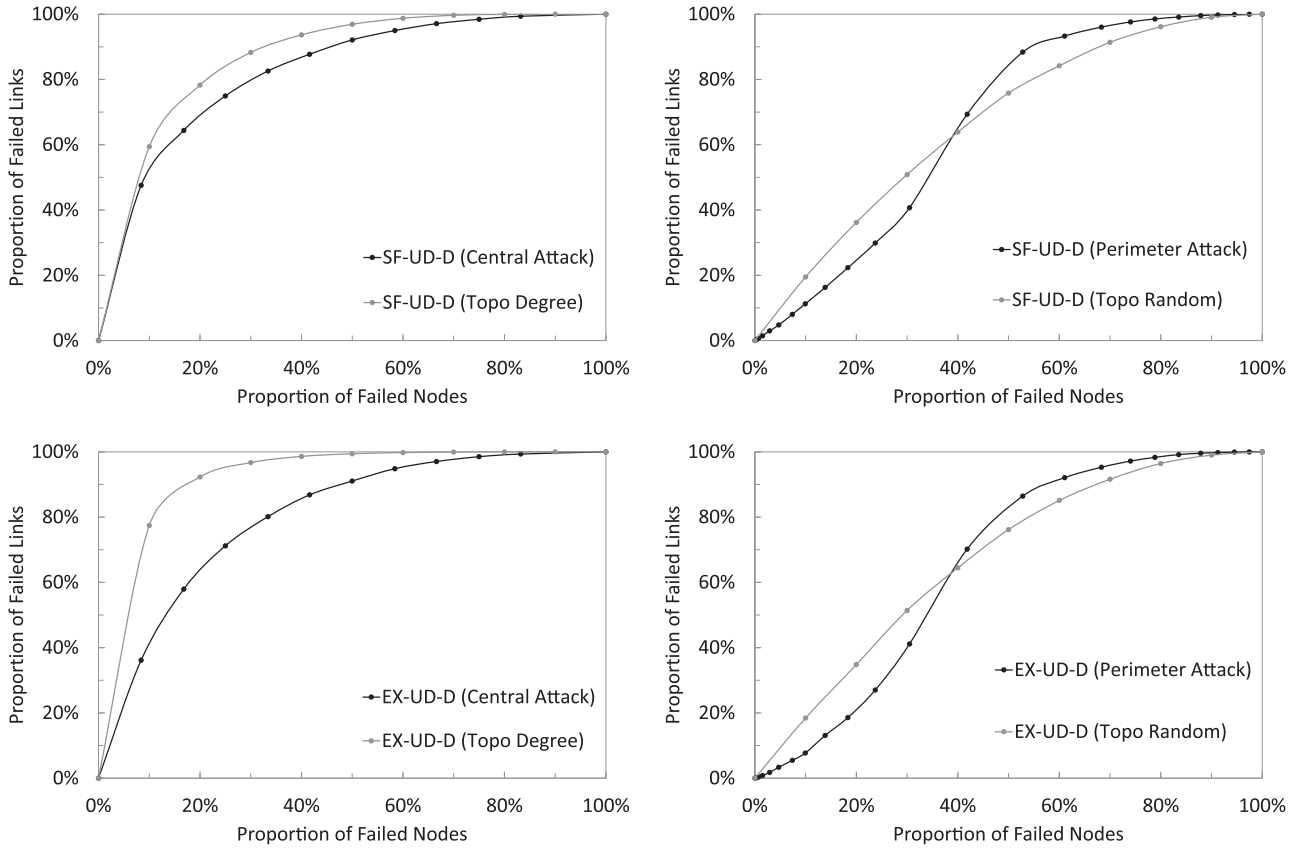

Fig. 9. Showing (a, c) the 'worst case' and (b, d) 'best case' spatial and topological hazards for the scale-free and exponential networks respectively. We identify the spatial hazard and network combination that produces the 'worst case' results to be the uniform with distance network where nodes are introduced with distance from the geographical centre when subjected to the 'central attack' hazard. And the 'worst case' topological hazard to be that which removes nodes in order of their degree, highest to lowest. We also identify to spatial hazard and network combination that produces the 'best case' results to be the uniform with distance network where nodes are introduced with distance from the geographic centre when subjected to the 'perimeter attack' spatial hazard and the 'best case' topological hazard, of those tested, to be the random attack.

Table 8
Comparison of the quantified resilience of scale-free and exponential networks, shown in Fig. 9(a) and (c) respectively.

Series	Modified RSVI
Resilience of SF-UD-D (central attack) compared to SF-UD-D (topo degree)	+4.88%
Resilience of EX-UD-D (central attack) compared to EX-UD-D (topo degree)	+13.17%

Table 9
Comparison of the quantified resilience of scale-free and exponential networks, shown in Fig. 9(b) and (d) respectively.

Series	Modified RSVI (from 0% to 35%)	Modified RSVI (from 35% to 100%)
Resilience of SF-UD-D (perimeter attack) compared to SF-UD-D (topo random)	+23.08%	−4.85%
Resilience of EX-UD-R (perimeter attack) compared to EX-UD-R (topo random)	+32.75%	−5.19%

topological properties of these networks also needs to be considered in order to gain the 'whole picture' of a networks resilience.

5.4. Implications for real-world networks

In this paper, we have so far considered the resilience of our synthetic benchmark networks to a range of spatial and topological hazards. However, the results from these networks also have many potentially important implications for real-world systems. We have considered a range of real-world infrastructure systems in this paper and have identified their "synthetic proxy" network (see Table 2). Therefore, we can now make several conclusions regarding their spatial hazard tolerance, much in the same way as traditional network theory forms conclusions regarding the topological hazard tolerance of a network by considering its network class.

Considering the location of the high degree, or hub, nodes in the networks our results indicate that six out of the seven real-world networks would be highly vulnerable to all sizes of spatial hazard located over their geographic centre. Only the US highway network would show a level of resilience to this location of spatial hazard, due to the random dispersion of high degree nodes throughout the network. This finding may be surprising, as it is expected that real-world systems would have a level of resilience to disruptive events. However, their spatial distribution of high degree nodes renders them vulnerable to hazards located over this area. In the case of real-world infrastructure systems, this property could lead to potentially devastating wide-scale social and economic impacts if this area was impacted by hazard.

A total of five real-world networks, considered in this paper, display a uniform with distance configuration and our results show that these networks can be expected to show an increased

vulnerability if the area around their geographic centre is affected by hazard. This is due to the high proportion of nodes (or infrastructure assets) in this region. Conversely, they will also show an increased resilience if the perimeter of the network is affected. This analysis has also shown that for the two real-world networks that show a uniform with area configuration their resilience, or vulnerability, to spatial hazard is governed by the location of their high degree nodes, as any location of hazard over these networks will remove approximately the same number of nodes.

Overall, the results of this paper have shown that, from the real-world networks considered (Table 2), the US Air Traffic Network should be the most resilient to spatial hazards (due to its uniform with area nodal configuration). However, as this network has an exponential degree distribution it is inherently vulnerable to hazards affecting the high degree nodes. Therefore, it can be concluded that both the spatial and topological characteristics of a network must be considered in any hazard tolerance, resilience or reliability analysis.

6. Conclusions

In this paper, we have considered the spatial hazard tolerance of a range of generic networks, in a similar manner to the topological study by Albert et al. [1]. To achieve this, we have presented a methodology to quantify the resilience of networks when subjected to hazard. To develop the spatial synthetic networks, we considered two spatial nodal configurations and three network generation algorithms. We assessed their resilience to two locations of a "growing" spatial hazard and also subjected them to two topological hazards.

We initially showed that the order in which nodes are introduced to the scale-free and exponential networks (in the network generation algorithms) has a significant impact upon their hazard tolerance, due to the placement of high degree nodes (Fig. 7). Networks where the nodes were introduced with distance from the geographic centre of the network were particularly vulnerable to hazards located over this area, being approximately 25% more vulnerable than the random benchmark networks (with an initial gradient of 5.66, compared to the random benchmark gradient of 1.96) (Tables 3 and 4). Networks where the high degree nodes were spatially dispersed (by introducing nodes at random locations to the network) were around 2% more resilient than the benchmark networks (using the modified RSVI value). This can be expected, as removing high degree nodes in a network will have more of an impact then removing lower degree nodes, however the significance of this paper is the quantification of these results.

We also considered the impact that nodal configuration has on the networks, finding that the uniform with distance nodal configuration was vulnerable to hazards located over the geographic centre of the network. In contrast, the uniform with area nodal configuration showed the same resilience to both locations of spatial hazard, due to the dispersion of nodes over the whole area, the modified RSVI measure showed that this nodal configuration is around 25% more resilient than the uniform with distance configuration (Table 6). Finally, it can be concluded that the spatial networks assessed in this paper showed a greater vulnerability to targeted topological hazard than the 'worst case' scenario of spatial hazard (being up to 13% more vulnerable as measured by the modified RSVI measure, Table 8). Whilst, the 'best case' combination of spatial network was up to 33% more resilient to a small scale random spatial hazard than the random topological hazard (Table 9).

In this paper, we also correlated the spatial and topological characteristics of a range of geographically distributed infrastructure systems with our generic networks. Of these networks we showed that five real world networks (European and China Air Traffic Networks, UK National Grid, US Rail Network and US Highway Network) displayed a uniform with distance nodal configuration and hence they are inherently vulnerable to even small spatial hazards located over their geographic centre. In contrast, the spatial hazard tolerance of the other two real-world networks, with a uniform with area configuration is governed by the location of the high degree nodes. This research has important implications for the analysis of real-world spatial networks in that a spatial hazard tolerance analysis must be carried out in addition to a topological assessment to fully understand the resilience of a network that has a significant or potentially governing, spatial component.

Acknowledgements

This research has been partly funded by an Engineering and Physical Sciences Research Council (EPSRC) Grant – "Resilient Electricity Networks for Great Britain" (RESNET) (EP/I035781/1).

References

[1] Albert R, Jeong H, Barabasi AL. Error and attack tolerance of complex networks. Nature 2000;406(6794):378–82.
[2] Amaral LAN, Scala A, Barthelemy M, Stanley HE. Classes of small-world networks. Proc Natl Acad Sci USA 2000;97(21):11149–52.
[3] Arenas A, Danon L, Diaz-Guilera A, Gleiser PM, Guimera R. Community analysis in social networks. Eur Phys J B 2003;38(2):373–80.
[4] Barabasi AL, Albert R. Emergence of scaling in random networks. Science 1999;286(5439):509–12.
[5] Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang DU. Complex networks: structure and dynamics. Phys Rep – Rev Sect Phys Lett 2006;424(4–5):175–308.
[6] Bullmore E, Sporns O. Complex brain networks: graph theoretical analysis of structural and functional systems. Nat Rev Neurosci 2009;10(3):186–98.
[7] Crucitti P, Latora V, Marchiori M. A topological analysis of the Italian electric power grid. Phys A – Stat Mech Appl 2004;338(1–2):92–7.
[8] CTA Railroad Network. Railroad network. ⟨http://cta.ornl.gov/transnet/RailRoads.html⟩; 2014 [retrieved 20.10.15].
[9] data.gov.uk. Network rail – inspire data. https://data.gov.uk/dataset/railway-network-inspire; 2015 [retrieved 05.10.15].
[10] Dunn S, Fu G, Wilkinson SM, Dawson R. Network theory for infrastructure systems modelling. Proc ICE – Eng Sustain 2013;166(5):281–92.
[11] Dunn S, Wilkinson SM. Understanding the fundamental resilience of lifelines. In: Proceedings of the second European conference on earthquake engineering and seismology. Turkey: Istanbul; 2014.
[12] Dunn S, Wilkinson S, Ford A. Spatial structure and evolution of infrastructure networks. Sustainable Cities and Society, in press, http://dx.doi.org/10.1016/j.scs.2016.08.011.
[13] Erdos P, Renyi A. On the evolution of random graphs. Publ Math Inst Hung Acad Sci 1960;5:17–61.
[14] Eusgeld I, Kröger W, Sansavini G, Schläpfer M, Zio E. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliab Eng Syst Saf 2009;94(5):954–63.
[15] Eusgeld I, Kroger W, Sansavini G, Schlapfer M, Zio E. The role of network theory and object-orientated modelling within a framework for the vulnerability analysis of critical infrastructures. Reliab Eng Syst Saf 2009;92(5):954–63.
[16] Eusgeld I, Nan C, Dietz S. "System-of-systems" approach for interdependent critical infrastructures. Reliab Eng Syst Saf 2011;96(6):679–86.
[17] Gastner MT, Newman MEJ. The spatial structure of networks. Eur Phys J B 2006;49(2):247–52.
[18] Gastner MT, Newman MEJ. Optimal design of spatial distribution networks. Phys Rev E 2006;74:1.
[19] Guimera R, Mossa S, Turtschi A, Amaral LAN. The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. Proc Natl Acad Sci USA 2005;102(22):7794–9.
[20] Treasury HM, Infrastructure UK. National infrastructure plan.London: The Stationery Office Limited; 2011.
[21] La Rovere S, Vestrucci P. Investigation of the structure of a networked system. Reliab Eng Syst Saf 2012;107:214–23.
[22] Lewis TG. Network science: theory and practice. John Wiley & Sons; 2009.
[23] Li D, Zhang Q, Zio E, Havlin S, Kang R. Network reliability analysis based percolation theory. Reliab Eng Syst Saf 2015;142:556–62.
[24] Li H, Guo XM, Xu Z, Hu XB. A study on the spaital vulnerability of the civil aviation network system in China. In: Proceedings of the IEEE 17th

international conference on intelligent transportation systems. Qingdao, China; 2014.
[25] Magnien C, Latapy M, Guillaume JL. Impact of random failures and attacks on Poisson and power-law random networks. ACM Comput Surv 2011;43(3).
[26] Newman MEJ, Watts DJ, Strogatz SH. Random graph models of social networks. Proc Natl Acad Sci USA 2002;99:2566–72.
[27] Openflights. OpenFlights.org. ⟨http://openflights.org/⟩; 2010 [retrieved 13.08.10].
[28] Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 2014;121:43–60.
[29] Ouyang M, Wang Z. Resilience assessment of interdependent infrastructure systems: with a focus on joint restoration modeling and analysis. Reliab Eng Syst Saf 2015;141:74–82.
[30] Ouyang M, Pan Z, Hong L, He Y. Vulnerability analysis of complementary transportation systems with applications to railway and airline systems in China. Reliab Eng Syst Saf 2015;142:248–57.
[31] Pant R, Hall J, Barr S, Alderson D. Spatial risk analysis of interdependent infrastructures subjected to extreme hazards. Vulnerability Uncertain Risk 2014:677–86.
[32] Rosas-Casals M, Valverde S, Sole RV. Topological vulnerability of the European power grid under errors and attacks. Int J Bifurc Chaos 2006;17(7):2465–75.
[33] Royal Academy of Engineering. Infrastructure engineering and climate change adaptation – ensuring services in an uncertain future, London; 2011.
[34] Rual J-F, Venkatesan K, Hao T, Hirozane-Kishikawa T, Dricot A, Li N, Berriz GF, Gibbons FD, Dreze M, Ayivi-Guedehoussou N, Klitgord N, Simon C, Boxem M, Milstein S, Rosenberg J, Goldberg DS, Zhang LV, Wong SL, Franklin G, Li S, Albala JS, Lim J, Fraughton C, Llamosas E, Cevik S, Bex C, Lamesch P, Sikorski RS, Vandenhaute J, Zoghbi HY, Smolyar A, Bosak S, Sequerra R, Doucette-Stamm L, Cusick ME, Hill DE, Roth FP, Vidal M. Towards a proteome-scale map of the human protein–protein interaction network. Nature 2005;437(7062):1173–8.
[35] Sporns O. Network analysis, complexity, and brain function. Complexity 2002;8(1):56–60.
[36] Stam CJ, Reijneveld JC. Graph theoretical analysis of complex networks in the brain. Nonlinear Biomed Phys 2007;1(3):1–19.
[37] Valverde S, Solé RV. Hierarchical small worlds in software architecture. Arxiv Prepr Cond-Mat/0307278 2003.
[38] Wilkinson S, Dunn S, Ma S. The vulnerability of the European air traffic network to spatial hazards. Nat Hazards 2012;60(3):1027–36.
[39] Zanin M, Lillo F. Modelling the air transport with complex networks: a short review. Eur Phys J – Spec Top 2013;215(1):5–21.